Department of Homeland Security Daily Open Source Infrastructure Report for 31 August 2006

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Daily Highlights

- VNUNet reports many of the used smart phones and PDAs for sale online contain sensitive data ranging from banking records to corporate e−mails that can easily be retrieved by hackers and data thieves. (See item 5)
- The Federal Aviation Administration sent its managers a memorandum nine months ago forbidding air traffic controllers in towers to be assigned solo, with responsibility for both radar and ground observations; yet this memo was not followed at Bluegrass Airport where a jet took a wrong turn to a too−short runway and then crashed. (See item 12)
- The BBC reports the latest research suggests that blood transfusions taken from people who have recovered from the H5N1 strain of bird flu might be an effective addition to the treatment arsenal, along with vaccines and anti−viral drugs. (See item 25)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 30, Platts Energy Bulletin* — **Argentina, South Africa plan to revive uranium enrichment programs.** Argentina and South Africa have announced plans to revive uranium enrichment programs mothballed since the last decade. Confirming a government

announcement August 23, Dario Jinchuk, head of international relations at the Argentine Nuclear Energy Commission (CNEA), said that CNEA hopes by the end of this year to restart its pilot gaseous diffusion plant at Pilcaniyeu. The goal, he said, is to have Argentina recognized as a commercial enricher on the world market in the framework of international initiatives to organize world nuclear fuel supply. South Africa's energy minister, Buyelwa Sonjica, told a meeting of young nuclear professionals on August 25, that the government intends to conduct a cost−benefit study aimed at reviving uranium enrichment at Pelindaba.
Source: http://www.platts.com/Nuclear/News/8609769.xml?p=Nuclear/News&sub=Nuclear&src=energybulletin

2. *August 30, Reuters* — **OPEC president says current oil price is satisfactory.** The current price of crude oil at $70 a barrel is satisfactory to the Organization for the Petroleum Exporting Countries (OPEC) and is not damaging world economic growth, the president of the exporters' group said Wednesday, August 30. Edmund Daukoru of Nigeria said world prices had subsided from record levels around $80 due to the ceasefire between Israel and Lebanon, a benign hurricane season in the Gulf of Mexico and some recovery in Nigerian production. The priority of OPEC is to reduce volatility rather than target a specific price range, Daukoru added, declining to specify a price level at which OPEC would cut production. The 11−member cartel is producing close to its full capacity, with only Saudi Arabia holding back spare volumes. It meets on September 11 in Vienna, Austria. Daukoru also said he had begun talks with fellow members about the difficult issue of OPEC Secretary General, which has been deadlocked since 2003 between Iran and Kuwait. The selection process for the administrative post, which represents the organization and helps coordinate policy talks among members, often reveals political divisions in the cartel. All decisions in OPEC must be unanimous.
Source: http://www.usatoday.com/money/industries/energy/2006−08−30−OPEC−prez_x.htm

3. *August 29, USA TODAY* — **Gasoline prices could keep falling.** Gasoline prices are falling fast and could keep dropping for months. The only place they have to go is down," says Fred Rozell, gasoline analyst at the Oil Price Information Service . "We'll be closer to $2 than $3 come Thanksgiving." Travel organization AAA foresees prices 10 cents a gallon lower by the end of next week. It reported a nationwide average of $2.84 Tuesday, August 29, the lowest since April 20. It's good news for consumers and the economy. Continued lower prices "may act like a tax cut" and stimulate spending, says Richard DeKaser, chief economist at National City in Cleveland. He calculates that higher energy prices the first six months cut growth of consumer spending one percentage point.
Source: http://www.usatoday.com/money/industries/energy/2006−08−29−gas−price−usat_x.htm

4. *August 29, Puget Sound Business Journal (WA)* — **Washington natural gas bills to go up 10 percent, says PSE.** Puget Sound Energy (PSE) said rising natural gas costs will force it to increase prices by about 10 percent beginning October 1. PSE, a subsidiary of Bellevue, WA−based Puget Energy Inc. filed a rate request with the state Utilities and Transportation Commission that would raise the monthly gas bill of a typical residential customer by about 8.7 percent, or $7.26. Officials at PSE said prices "rose significantly" in the past year, due to severe damage caused by hurricanes in the Southeast and increased demand.
Source: http://biz.yahoo.com/bizj/060829/1338278.html?.v=1

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *August 30, VNUNet* — **PDAs sold on eBay loaded with sensitive data.** Many of the used smart phones and PDAs for sale online are loaded with sensitive data ranging from banking records to corporate e−mails that can easily be retrieved by hackers and data thieves. According to a sampling by mobile security software provider Trust Digital, much of this sensitive information is retained in the Flash memory of the devices because of a widespread failure to perform the advanced hard reset required to delete data. Trust Digital claimed that its engineers were able to recover nearly 27,000 pages of personal, corporate and device data from nine out of 10 mobile devices purchased through eBay for the project.
   Source: http://www.vnunet.com/vnunet/news/2163176/pdas−sold−ebay−loa ded−sensitive

6. *August 29, CNN Money* — **Hackers steal personal information of 19,000 AT&T customers.** Personal data, including credit card information, of 19,000 AT&T customers was stolen by hackers over the weekend, the company reported late Tuesday, August 29. The breach, which affected customers who purchased DSL equipment through AT&T's (Charts) Web store was discovered within hours and the online store was shut down immediately. AT&T said it would pay for credit monitoring services for the affected customers.
   Source: http://money.cnn.com/2006/08/29/news/companies/att/

7. *August 29, Tech Web* — **Bank to pay $50 million for buying personal data.** A bank has been ordered to pay a $50 million settlement for buying more than 650,000 names and addresses from the Florida Department of Highway Safety and Motor Vehicles. The Electronic Privacy Information Center (EPIC) announced the decision this week. EPIC said Fidelity Federal Bank & Trust bought 656,600 names and addresses for use in direct marketing and the purchase violated the Drivers Privacy Protection Act.
   Source: http://www.techweb.com/wire/security/192500110

8. *August 29, WXIA−TV Atlanta* — **Identity theft scam in Georgia involves fast−food chains.** Takelia Anderson, a female employee working the drive−thru window at Taco Bell in Smyrna, GA, stole customers' identities by swiping their credit and debit cards with a skimmer. Police say Anderson was recruited by Arthur Crumpley. Crumpley recruited fast food workers around Atlanta, promising them $1,000 for every 50 card numbers stolen. Police say they believe the

scam is occurring across Metro Atlanta.
Source: http://www.11alive.com/news/news_article.aspx?storyid=83996

9. *August 29, Finextra (UK)* — **Canadian phishers in pump−and−dump probe.** Canadian regulators are investigating a rash of phishing frauds at online brokerages in which raiders used the funds from looted accounts to artificially inflate the price of penny stocks. The Investment Dealers Association of Canada has warned brokerages to be on the alert for suspect account activity after a number of member firms reported the scams, in which customer accounts were liquidated and the funds used to place orders for specific securities listed on the OTC Bulletin Board and the Nasdaq pink sheets. A number of customers of BMOInvestorLine were hit by the crooks, while TD Waterhouse is also investigating a rash of similar incidents.
Source: http://www.finextra.com/fullstory.asp?id=15778

10. *August 29, Tech Web* — **Scammers jump on "Ernesto" domain names.** Possible scammers have been busy registering domains with the name "Ernesto," the SANS Institute's Internet Storm Center said Tuesday, August 29. A year ago, criminals registered a large number of Hurricane Katrina−related Websites and solicited donations from Web users. As of early Tuesday, 19 new domains with the term "Ernesto" have come online. Of the 19, 18 are hurricane related; 17 of those were registered by one person.
Source: http://www.techweb.com/wire/security/192500033;jsessionid=ZBQ3MWOOTHVLMQSNDLRSKHSCJUNN2JVN

11. *August 29, Department of the Treasury* — **Department of the Treasury designates key Hezbollah fundraising organization.** The Department of the Treasury on Tuesday, August 29, designated the Islamic Resistance Support Organization (IRSO), a key Hezbollah fundraising organization. "While some terrorist−supporting charities try to obscure their support for violence, IRSO makes no attempt to hide its true colors. IRSO's fundraising materials present donors with the option of sending funds to equip Hezbollah fighters or to purchase rockets that Hezbollah uses to target civilian populations," said Stuart Levey, Department of the Treasury's Under Secretary for Terrorism and Financial Intelligence.
Source: http://www.treasury.gov/press/releases/hp73.htm

[Return to top]

Transportation and Border Security Sector

12. *August 30, New York Times* — **FAA memo on controllers wasn't followed in Lexington.** The Federal Aviation Administration (FAA) sent its managers a memorandum nine months ago forbidding air traffic controllers in towers to be assigned solo, with responsibility for both radar and ground observations. But the policy was not followed at Bluegrass Airport, where a jet took a wrong turn to a too−short runway on Sunday, August 27, and crashed before the lone controller noticed the error. The memorandum was sent last November, after an overloaded controller at the Raleigh−Durham airport in North Carolina directed two planes to be too close. Internal documents show that the air traffic manager at Bluegrass Airport was trying to solve the staffing problem on the overnight shift by getting radar responsibility transferred to a round−the−clock center in Indianapolis that handles mostly high−altitude traffic, but he did not

succeed. Laura J. Brown, a spokesperson for the FAA, said that the November edict was not a new policy, and that it was seeking to enforce a longstanding policy that had somehow fallen into disuse. The agency's headquarters learned of the staffing situation at Bluegrass only after the Sunday crash, Brown said.
Source: http://www.nytimes.com/2006/08/30/us/30crash.html?ref=us

13. *August 30, United Press International* — **Iraqi barred from NYC flight over t−shirt.** Security officials at New York's John F. Kennedy International Airport refused to allow a man to board his flight because of an Arabic inscription on his t−shirt. Iraqi−born architect Raed Jarrar said security staff told him his t−shirt, which said, "We will not be silent" in Arabic and English was upsetting other passengers, New York Public Radio, reported on Wednesday, August 30. Jarrar ended up putting on another t−shirt provided by Jet Blue airline staff over the original one.
Source: http://www.upi.com/NewsTrack/view.php?StoryID=20060830−10295 9−6583r

14. *August 30, NBC5 (IL)* — **Hazmat crews called to O'Hare airport overnight.** There was a flurry of activity at Chicago's O'Hare International Airport overnight as officials responded to a report of an unknown material found near an aircraft. The source and identity of the product were not known, but FBI, fire, police, bomb and arson investigators were called to the scene very early on Wednesday, August 30. The incident occurred in a United maintenance hanger, far from passengers and flight crews, and at no time, were travelers in any danger.
Source: http://www.nbc5.com/news/9760407/detail.html

15. *August 30, Department of Transportation* — **United States, Kuwait sign Open−Skies aviation agreement.** The United States and Kuwait today agreed to remove all barriers limiting the number and range of commercial airline flights between the two countries. The agreement, known as an Open−Skies agreement, means U.S. and Kuwaiti airlines will be free to set service schedules and prices between the two countries based on travel demand. U.S. Ambassador Richard LeBaron and Kuwait,s Director of Civil Aviation Yacoob Al−Saqer signed the agreement in Kuwait City. Both sides agreed to apply the terms of the agreement immediately, pending ratification by the Kuwaiti Parliament. Open−Skies agreements permit unrestricted air service by the airlines of both sides between and beyond the other's territory, without restrictions on how often the carriers can fly, the prices they charge, or the kind of aircraft they use. The accord with Kuwait also will allow all−cargo carriers to fly between the other country and third countries without directly connecting to their homeland. Although this is the first air services agreement between the two countries, Kuwait Airways has served the United States since 1978 by the mutual agreement of the two governments. The United States now has Open−Skies relationships with 77 aviation partners, including six in the Middle East.
Source: http://www.dot.gov/affairs/dot8906.htm

16. *August 30, American City Business Journal* — **Kentucky airport gets money for taxiway extension and emergency operations center.** The Federal Aviation Administration has given the Louisville Regional Airport Authority approval to begin construction of a planned taxiway near the United Parcel Service Inc. (UPS) Worldport hub at the Louisville International Airport. The taxiway is necessary to accommodate the large Airbus A380 aircraft, which UPS plans to begin flying into the hub by the end of the decade. The A380 has a wingspan of nearly 262 feet, a height of 80 feet and a length of 239 feet. Bids have been accepted, and a contract might be

awarded at the September airport authority board meeting, said Skip Miller, executive director of the airport authority.
Source: http://louisville.bizjournals.com/louisville/stories/2006/08 /28/daily24.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

17. *August 30, Animal and Plant Health Inspection Service* — **Final rule regarding bovine tuberculosis for Minnesota adopted.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service has adopted, without change, an interim rule amending bovine tuberculosis (TB) regulations by removing Minnesota from the list of accredited−free states and adding it to the list of modified accredited advanced states. This rule is necessary to help prevent the spread of bovine TB because Minnesota no longer meets the requirements for accredited−free state status. Minnesota identified three affected herds in 2005 and two in 2006. In addition, two infected, wild, white−tailed deer were found in close proximity of one of the index herds. Minnesota is performing epidemiologic investigations and testing for all herds linked to the five affected herds in the state. In accordance with federal regulations, Minnesota has written a TB management response plan that calls for wider surveillance regarding TB in cattle, wild deer, outreach and educational initiatives for shareholders. If Minnesota completes all requirements in the federal regulations and find no more infection in livestock, they would be eligible to regain accredited−free status for TB in January 2008. Bovine TB is a contagious and infections disease caused by Mycobacterium bovis. It affects cattle, bison, deer, elk, goats and other warm−blooded species and can be fatal.
Source: http://www.aphis.usda.gov/newsroom/content/2006/08/mntbzone. shtml

18. *August 30, Animal and Plant Health Inspection Service* — **Oral rabies vaccine distributed in three states.** Wildlife Services, a program within the U.S. Department of Agriculture's Animal and Plant Health Inspection Service will distribute oral rabies vaccine baits in cooperation with state agriculture, health and natural resource agencies beginning on or about September 5, to prevent the spread of raccoon rabies in portions of Ohio, Pennsylvania and West Virginia. Baits containing oral rabies vaccine will be distributed over rural areas using low−flying twin−engine aircraft and hand baiting will occur in populated regions using ground−based vehicles. The projected two−week program will target raccoons and result in the distribution of more than two million baits covering roughly 14,000 total square miles in three states. In July 2004, a raccoon in Lake County, OH, tested positive for rabies about seven miles west of the existing vaccination barrier. An intense, oral rabies vaccination campaign is ongoing in the 20−mile radius surrounding the positive case.
Source: http://www.aphis.usda.gov/newsroom/content/2006/08/rabiohpa0 6.shtml

19.

August 29, Agriculture Online — **Sudden death syndrome showing up in southern Minnesota.** Symptoms of sudden death syndrome (SDS) are appearing in southern Minnesota soybean fields. SDS first appeared in Minnesota in 2002. The disease has occurred most frequently in scattered locations in south−central Minnesota, says Dean Malvick, plant pathologist with University of Minnesota Extension. SDS symptoms are typically reported to develop in Minnesota in early− to late−August. "It's hard to predict when, where, and how severe SDS will become," said Malvick. "Many things influence disease development." According to Malvick, some factors that seem to favor development of SDS in the Midwest include: compacted soil and poor drainage, moderate to high populations of Soybean Cyst Nematode, wet soil conditions after planting, environments favorable for high soybean yields, soybean varieties with poor ratings for SDS resistance, early planting, and heavy rainfalls throughout the summer.
Sudden Death Syndrome of Soybean In Minnesota:
http://www.extension.umn.edu/cropenews/2006/06MNCN50.htm
Source: http://www.agriculture.com/ag/story.jhtml?storyid=/templatedata/ag/story/data/1156887553769.xml&catref=ag1001

[Return to top]

Food Sector

20. *August 25, Orange County Register (CA)* — **Two more people sick after eating live or raw crabs.** Two more people have been diagnosed with a rare parasitic infection after eating live freshwater crabs, the Orange County, CA, Health Care Agency said Thursday, August 24. In all, four diners have been reported sickened from eating live or raw crabs that were served at Riptide Sushi in Mission Viejo and Chomp Sushi in Fullerton, according to county officials. The rare lung infection is treatable with medication, though symptoms may not occur for six to 10 weeks after consumption. The sawagani or regal crabs carried the parasite paragonimus. Last week, the California Department of Health Services issued a statewide warning that restaurants in 16 counties had received the crabs. No cases have been found outside Orange County, spokesperson Patti Roberts said.
Source: http://www.ocregister.com/ocregister/homepage/abox/article_1 254628.php

[Return to top]

Water Sector

21. *August 30, Associated Press* — **Water shortage brings hotel closure order in Canadian resort town.** Hotels, resorts and other businesses in Tofino, British Columbia, a rainforest tourist Mecca on Vancouver Island, have been told to shut down due to a water shortage. Because of high demand and very little rain since July, the town's main reservoir is so depleted that there might not be enough water to fight a fire, Mayor John Fraser said Tuesday, August 29. A notice said residential water service was being given priority in the town of 1,500 year−round residents at the western end of the Trans−Canada Highway. "The water shortage has become extremely severe," the notice read. "All lodging, food service businesses are asked to shut down PRIOR TO Friday, September 1, 2006 until further notice. Other commercial

water users must not consume any water whatsoever."
Source: http://seattlepi.nwsource.com/local/6420AP_WA_Tofino_Water.h tml

[Return to top]

Public Health Sector

22. *August 30, Food and Agriculture Organization* — **Helping prevent avian influenza in Latin America and the Caribbean.** In order to help prevent a possible outbreak of avian flu in Latin America and the Caribbean and enhance public awareness of the threat posed by the disease, the Food and Agriculture Organization (FAO) has just published a new handbook targeted especially to the region's small−scale poultry farmers. The publication, entitled Guide to the prevention and control of avian flu in small−scale poultry farming in Latin America and the Caribbean stresses the measures needed to ensure on−farm biosecurity and prevent contact between domestic poultry and potentially infected wild birds. FAO's handbook will also be circulated among the staff of local veterinary services and livestock technicians working with small−scale producers in Latin America and the Caribbean. The book grew out of a similar publication aimed at small−holders in Southeast Asia, a region where there was a massive outbreak of the deadly H5N1 virus in 2003/4 and from where it subsequently spread to Europe, the Near East and Africa.
Source: http://www.fao.org/newsroom/en/news/2006/1000381/index.html

23. *August 30, Xinhua (China)* — **Chinese bird flu vaccine developer to prepare for mass production.** A Chinese vaccine developer announced on Tuesday, August 29, it will expand production facilities to produce massive quantities of human bird flu vaccine once the drug passes two more rounds of clinical trials. After the expansion, which is expected to take six months, the company will increase its annual production from eight million vaccines to 20 million. The company developed the human bird flu vaccine together with China's Ministry of Science and Technology, and China Disease Control and Prevention Center. Preliminary clinical tests have shown that the vaccine is safe and effective for human use, researchers said. Results from the first−phase trails, which ended in June, showed the 120 people who were vaccinated had no serious adverse reactions. In China, a vaccine is allowed to enter the market after it completes three phases of clinical trials.
Source: http://english.people.com.cn/200608/30/eng20060830_298011.ht ml

24. *August 30, Reuters* — **Five in Indonesia's Sulawesi tested for bird flu.** Five people have been admitted to hospital on Indonesia's Sulawesi Island with bird flu−like symptoms and local authorities have sought funds from the government to help cull poultry, officials said on Wednesday, August 30. Samples from the patients in Palu, the capital of Central Sulawesi province, have been sent to a government laboratory in Jakarta to be tested for bird flu, said Runizar Ruesin, head of the ministry's bird flu information center. Indonesia has so far recorded 60 bird flu cases, 46 of them fatal. The country's death toll is the highest in the world. Zulkarnain Hassan, a coordinator at the agriculture ministry's Avian Influenza Crisis Centre, said that there had been bird flu cases in poultry in West and South Palu district and the provincial capital of Palu city.
Source: http://today.reuters.com/News/CrisesArticle.aspx?storyId=JAK 37876

25. *August 29, BBC* — **Transfusions may cut flu deaths.** Transfusions of blood products might help to cut deaths in a future flu pandemic, research suggests. Researchers examined records from the Spanish flu pandemic of 1918−1920 which killed up to 100 million worldwide. They found transfusions taken from people who had recovered may have improved the condition of others hospitalized by the virus. Experts fear that the H5N1 strain of bird flu responsible for the deaths of 140 people in Asia since 2003 could mutate to gain the ability to pass easily from human to human. The latest research suggests that blood transfusions might be an effective addition to the treatment arsenal, alongside vaccines and anti−viral drugs. The World Health Organization has warned the world is not ready for a flu pandemic, and that a vaccine will take time to prepare and distribute following the first outbreaks. Anti−viral drugs might also initially be in short supply. The researchers say a single recovering patient could donate enough blood plasma to treat many others.
Meta−Analysis: Convalescent Blood Products for Spanish Influenza Pneumonia: A Future H5N1 Treatment?: http://www.annals.org/cgi/content/full/0000605−200610170−001 39v1
Source: http://news.bbc.co.uk/1/hi/health/5294378.stm

[Return to top]

Government Sector

26. *August 30, CNN* — **Two injured in North Carolina school shooting.** A student was shot in the shoulder after a suspect fired eight shots toward a Hillsborough, NC, high school, police said. According to WTVD−TV, Orange County deputies have the suspect in custody. The male suspect drove to Orange High School about 1 p.m. EDT and didn't stop for school security. He got out of his vehicle and fired the shots, striking the female student in the shoulder. Another male student was injured by broken glass, the television station reported. Orange High School and nearby Stanford Middle School were both put on lockdown, and parents were not being allowed at the schools, according to WTVD. Orange High has 1,009 students in grades nine through 12.
Source: http://www.cnn.com/2006/US/08/30/school.shooting/index.html

[Return to top]

Emergency Services Sector

27. *August 30, Washington Times (DC)* — **Computer game will train first responders.** A Maryland company has developed a computer game to train emergency responders who are forced to make life−and−death decisions in the blink of an eye. The game, Incident Commander, simulates crisis scenarios including a severe storm, a natural disaster, a school hostage situation and a terrorist attack. It was developed for the Department of Justice as part of the National Incident Management System mandated after the September 11 attacks. As many as 16 players can train simultaneously on computers at work or from home, assuming the role of the commander or a member of the operations team. The game simulates the chaos of emergency situations. For example, the game's severe−storm scenario challenges players with broken water mains, gas leaks, destroyed buildings, obstructed roads and injured civilians. Users can customize the simulation according to their locality. The scenarios compress days

and weeks into games lasting several hours. Users can play from start to finish or pause and complete the simulation during multiple sessions. The game scores players on public safety, based on how many civilians are killed or injured; media, or how the incident played out on television; and total cost of the response.
Source: http://washingtontimes.com/business/20060829−093839−3370r.ht m

28. *August 30, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: At 5:00 am EDT Wednesday, August 30, the center of Tropical Storm Ernesto was located in northeastern mainland Monroe County, FL. This is also about 45 miles west−southwest of Miami, FL and about 90 miles south−southwest of West Palm Beach, FL. Ernesto is moving toward the north−northwest near 8 mph. A turn to the north with an increase in forward speed is expected later today. The center of Ernesto is expected to remain over the Florida Peninsula for the next day or so. Maximum sustained winds are near 45 mph with higher gusts. Some weakening is possible due to the center of circulation remaining over the Florida Peninsula and Ernesto could weaken to a Tropical Depression later today. However, rainbands containing strong gusty winds to tropical storm force will continue to move onshore today in the warning areas especially along the Florida East Coast.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat083006.shtm

29. *August 28, Chicago Sun−Times* — **Evacuation drill scheduled for downtown Chicago.** Emergency preparedness officials in Chicago will stage a “voluntary evacuation” of fewer than a dozen buildings in a section of the Loop that Chief Emergency Officer Cortez Trotter described as “two square blocks, maybe more.” The drill is tentatively scheduled for Thursday, September 7. Building employees who agree to participate will be directed to designate “transport centers,” Trotter said. From there, they will presumably be taken by bus to central gathering places where they will be given food, water, washcloths, toothbrushes, blankets and other essentials. The goal of the drill is to test in a real−life situation how prepared Chicago is for a mass evacuation nearly five years to the day after the September 11 terrorist attacks. The Loop evacuation drill is just one of several activities planned for National Preparedness Month. City Hall is also planning public service announcements and presentations at schools and senior citizen centers to spread the word about disaster preparedness and the need to make advance plans to protect children, the elderly and pets.
Source: http://www.suntimes.com/output/news/evac28.html#

30. *August 08, Department of Homeland Security, Office of Inspector General* — **DHS releases audit report on FEMA’s search and rescue teams.** The Department of Homeland Security’s (DHS) inspector general’s office released a report on their audit of the National Urban Search and Rescue Response System (US&R System), which is under the administration of the Federal Emergency Management Agency (FEMA). While the US&R System has made improvements, the report stated that the task forces are falling short in achieving US&R System objectives and standards in three primary areas of readiness: operational, logistical, and management. Due to funding shortages and staffing constraints, FEMA did not monitor the task forces' compliance with grant agreement requirements or their achievement of US&R System objectives and standards for optimal task force response preparedness. There were also delays in FEMA’s hiring of full–time staff to administer day−to−day activities, budget constraints, and US&R

System management staff shortages. The report recommended that FEMA take steps to improve the administration, funding, and oversight of the federally funded task forces.
Source: http://www.dhs.gov/interweb/assetlibrary/OIG_06−54_Aug06.pdf

[Return to top]

Information Technology and Telecommunications Sector

31. *August 30, Sophos* — **Graphic e−mail points to malicious Trojan horse.** Sophos experts based in Sydney have discovered e−mail messages are being sent to Australian computer users claiming to come from a young woman visiting the country. Unusually, the malicious e−mails contain no text, but an embedded graphical image telling users to visit a Website. The Website referred to in the e−mail contains a soft porn image and a link to the Troj/Dloadr−AMA Trojan horse.
Source: http://www.sophos.com/pressoffice/news/articles/2006/08/vick y−image−trojan.html

32. *August 29, Security Focus* — **Multiple Microsoft vulnerabilities reported.** A vulnerability has been discovered in Microsoft Internet Explorer that is prone to a memory corruption vulnerability. Analysis: This issue may be exploited when an attacker use a malicious Webpage to execute arbitrary code in the context of the currently logged in user. Exploitation attempts may lead to a denial−of−service condition as well. Attacker may also employ HTML e−mail to carry out an attack.
For further detail: http://www.securityfocus.com/bid/19570/discuss
Microsoft Internet Explorer is prone to a denial−of−service vulnerability that occurs when instantiating Visual Studio COM objects. Analysis: This vulnerability arises due to the way Internet Explorer tries to instantiate certain COM objects as ActiveX controls, resulting in denial−of−service conditions. Remote code execution may be possible, but have not been confirmed.
For further detail: http://www.securityfocus.com/bid/19572/discuss
Microsoft Windows DHCP Client fails to properly bounds check user supplied input before copying it to an insufficiently memory buffer, which leaves it prone to a remote code execution vulnerability. Analysis: This vulnerability allows remote attackers to execute arbitrary machine code with SYSTEM−level privileges on affected computers. This facilitates the complete compromise. Please see source for further detail.
Source: http://www.securityfocus.com/bid/18923/discuss

33. *August 29, Security Focus* — **AOL Security Edition local privilege escalation vulnerability.** AOL Security Edition is prone to a local privilege escalation vulnerability. This vulnerability arises because of insecure default permissions associated with directories, which can allow local attackers to place arbitrary executables in a directory that may be executed with elevated privileges.
Vulnerable: AOL Security Edition 9.0.
Solution: AOL has released fixes to address this issue. These fixes can be automatically applied by logging into the service.
Source: http://www.securityfocus.com/bid/19583/references

34. *August 29, eSecurityPlanet* — **Clagge.B Trojan downloads other Trojan.** Clagge.B is a Trojan that downloads Trj/Banker.CZI from a certain Website to the affected computer. Additionally, it bypasses Windows XP firewall. Clagge.B does not spread automatically using its own means. It needs an attacking user's intervention in order to reach the affected computer. For further detail: http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?lst=det&idvirus=127950
Source: http://www.esecurityplanet.com/alerts/article.php/3629146

35. *August 29, Sophos* — **Sdbot−COL Worm and Trojan targets weak passwords.** W32/Sdbot−COL is a spyware worm and IRC backdoor Trojan that spreads via network shares with weak passwords and affects the Windows operating system. The side effects of this worm includes: a) allows others to access the computer; b) steals information; c) downloads code from the Internet; d) installs itself in the Registry. Two aliases of this worm includes W32.Gaobot.SN and WORM_RBOT.GN.
Source: http://www.sophos.com/security/analyses/w32sdbotcol.html

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4672 (eMule), 139 (netbios−ssn), 445 (microsoft−ds), 80 (www), 113 (auth), 25 (smtp), 6346 (gnutella−svc), 1433 (ms−sql−s), 135 (epmap) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

36. *August 30, Associated Press* — **Police to install 12 neighborhood cameras.** Washington, DC, police are installing a dozen surveillance cameras in city neighborhoods. The cameras were authorized in the emergency crime legislation passed by the DC Council earlier this summer. Police say officers won't usually be monitoring them in real time, but will watch replays of the video they record while investigating crimes. Installation began Monday, August 28, and should be completed by the end of the week. Police Chief Charles Ramsey chose the locations of the cameras based on calls for service, reported crimes, and recommendations and requests from the Advisory Neighborhood Commissions and other neighborhood groups.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=51726

[Return to top]

General Sector

37. *August 30, Washington Post* — **FBI shows off counterterrorism database.** The FBI has built a database with more than 659 million records −− including terrorist watch lists, intelligence cables and financial transactions −− culled from more than 50 FBI and other government agency sources. The system is one of the most powerful data analysis tools available to law enforcement and counterterrorism agents, FBI officials said Tuesday, August 29. The Investigative Data Warehouse, launched in January 2004, is an effort to "connect the dots" that the FBI was accused of missing in the months before the 2001 attacks, bureau officials said. About a quarter of the information comes from the FBI's records and criminal case files. The rest comes from the Treasury, State and Homeland Security departments and the Federal Bureau of Prisons. "That's where the real knowledge comes from...sharing information," said Gurvais Grigg, acting director of the FBI's Foreign Terrorist Tracking Task Force, who helped develop the system. The system can be programmed to send alerts to agents on new information, Grigg said. Names, Social Security numbers and driver's license details can be linked and cross−matched across hundreds of millions of records.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/08/29/AR2006082901520.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer